# Mpumalanga Provincial Government

OMNIA LABOR VINCIT

## Department of Public, Works Roads and Transport

## INFORMATION TECHNOLOGY (IT) POLICY

Revision Date:...............................................................................None
Issue: ...............................................................................1.0
Responsible Section............................................................................ Knowledge Management
Approval Date......................................................................

# TABLE OF CONTENTS

## TABLE OF CONTENTS

# ABBREVIATIONS AND DEFINITIONS

## ABBREVIATIONS

| | | |
|---|---|---|
| **AUP** | : | Acceptable Use Policy |
| **DITC** | : | Departmental Information Technology Committee |
| **DRP** | : | Disaster Recovery Plan |
| **E-MAIL** | : | Electronic Mail |
| **ETC** | : | Et cetera |
| **FTP** | : | File Transfer Protocol |
| **GCCN** | : | Government Common Core Network |
| **GIS** | : | Geographic Information System |
| **GM** | : | General Manager |
| **HOD** | : | Head of Department |
| **I &RM** | : | Information and Records Manager |
| **IS** | : | Information Systems |
| **ISS** | : | Information and Security Systems |
| **IT** | : | Information Technology |
| **ITB** | : | Information Technology Bureau |
| **LAN** | : | Local Area Network |
| **MISS** | : | Minimum Information Systems Security |
| **MPG** | : | Mpumalanga Provincial Government |
| **NDA** | : | Non-Disclosure Agreement |
| **PC** | : | Personal Computer |
| **PIN** | : | Personal Identification Number |
| **PKI** | : | Public Key Infrastructure |
| **PWR&T** | : | Department of Public Works, Roads and Transport |
| **SACSA** | : | South African Communication Security Agency |
| **SITA** | : | State Information Technology Agency |
| **SLA** | : | Service Level Agreement |

| | | |
|---|---|---|
| **WAN** | : | Wide Area Network |
| **WWW** | : | World Wide Web |

## DEFINITIONS

**IT Solutions** All IT Hardware and Software resources e.g. Personal computers, laptops, printers, Systems and all other IT-related Services.

**Local Area Network** A group of computers connected as on a network. A communication infrastructure that enables users to share resources such as printers, software, data, etc in a way that is cost-effective.

**Monitoring** The actions directed at measuring performance to ensure the confidentiality, availability and integrity of systems and information.

**Information Systems** Applications and systems used to process data utilizing IT as an enabling tool.

**Information Technology** This refers to the processing of data via a computer/s. These are aspects of technology that are used to manage and support the efficient gathering, processing, storing and dissemination of information as a resource. Information Technology is a data processing enabler.

**IT Incident** Any event that has actual or potential effect on the information and information systems resulting in fraud, abuse and loss.

**Password** Security code or pin code

**Server** File server or Document server

**SITA** An Agency of State established in 1999 through a special act of parliament to consolidate and coordinate the State's Information Technology resources.

**System Owner** A business manager (not necessarily an IT professional) with the ultimate responsibility on the system. The system owner allocates system resources, sets objectives and ensures integrity and quality of the system.

**User** A person using computer equipment and network resources of the Department of Public Works, Roads & Transport

**Consultant** A person or company engaged by the Department to do business on their behalf

**Illegal** Lacking permission and not authorized

**Cryptography** The science of transforming information into unreadable format (or the encryption of data)

## 1. INTRODUCTION

The purpose of this policy is to enable the Department of Public works, Roads and Transport (PWR&T) to apply an effective and consistent level of security to all its information and information systems.

Every organization depends on information as a vital asset to make informed decisions.

The Department critically depends on information and information systems and seeks to protect its information and information systems from loss, misuse and damage.

Through this policy, the Department seeks to ensure that the **confidentiality**, **integrity** and **availability** of its information are maintained by implementing best practices to minimize any potential risk to information.

Failure to comply with this policy shall be considered as misconduct and depending on the circumstances and seriousness of the offence, appropriate disciplinary action shall take place.

**1.1** The policy is based on the following profound security principles:**PRINCIPLES**

1.1.1 **Proportional Cost vs. benefit:** All security measures shall be appropriate and proportional to the cost and benefit of implementing such measures for which they are designed to protect.

1.1.2 **Adversary:** All security measures shall be established in the anticipation of natural disaster, harmful intent and hostile attack.

1.1.3 **Least Privilege:** Access to any IT system shall be granted on the basis of business need to access the facility in other words, the need-to-know basis.

1.1.4 **Separation of Duty:** Job functions shall be divided amongst co-workers. For example no one person shall have access to both add employees to the Human Resources System and authorise payment for these people. No one person shall have access to place an order and pay a supplier.

1.1.5 **Ethics:** In the implementation of the policy, the Department adheres to an ethical code of conduct in relation to monitoring and accessing of user accounts. An ethical judgement in this regard may need to be made.

1.1.6 **Timeliness:** Employees and Third Party/s shall act or respond within a reasonable time period to any identified risk or security breach.

1.1.7 **Confidentiality:** Unauthorised disclosure of information is prohibited.

1.1.8 **Integrity**: Unauthorised modification of information is prohibited.

1.1.9 **Availability**: Refers to both Data and Service. Data shall be accessible when required. Systems to have redundancy built in.

1.1.10 **Controlled Access:** Information assets shall only be used for business purposes and for the business purpose intended.

1.1.11 **Levels of Protection / Assurance of protection / multiplicity of protection:** In accordance with MISS, the following levels of classification shall determine the levels of protection –

1.1.11.1 Restricted

1.1.11.2 Confidential

1.1.11.3 Secret

1.1.11.4 Top Secret

1.1.12 **Protected measure baseline:** The Department information is an important asset that shall be protected according to its value and degree of damage that could result from its misuse, unavailability, destruction, unauthorised disclosure or modification. This implies that information assets shall be identified, valued, assessed for risk and protected cost effectively from identified threats in accordance with the principle of Cost Vs Benefit.

1.1.13 **Continuity of Protection:** The Department's information is an important asset that shall be protected on a 24/7/365 basis.

**1.1.14 System Stability:** The Department information is an important asset that shall be available as and when required. This shall entail a 24/7 unless otherwise specified via Change Management.

1.1.15 **Survivability:** The Department information is an important asset that shall have the ability to be sustained in the event of a disaster. Disaster Recovery Plans shall be established and structured walk-through testing shall be done. Implementation of the plans shall be managed on a project-to-project basis.

1.1.16 **Individual Accountability:** Every individual is accountable for the security of the departmental assets under their control. The delegation of responsibility for security is assigned to each and every user within the Department. Mechanisms such as Userld's are in place to ensure individual accountability.

## 2. OBJECTIVES

The purpose of this policy is to:

2.1 Promote information protection and Systems security

2.2 Protect information and information systems from loss, misuse and damage

2.3 Promote proper usage of IT solutions

2.4 Provide guidelines on the acquisition of IT solutions

## 3 REGULATORY FRAMEWORK

3.1 The Constitution of the Republic of South Africa of 1996.

3.2 Information Act 2002 (Act No. 70 of 2002)

3.3 State Information Technology Agency Act 1998 (Act No. 88 of 1998)

3.4 Electronic Communication and Transaction Act 2002 (Act No. 25 of 2002)

3.5 Communication Security Act 2002 (Act No. 68 of 2002)

3.6 Promotion of Access to Information Act 2000 (Act No. 2 of 2000)

3.7 Copy Right Act 1978 (Act No. 98 of 1978)

3.8 Public Finance Management Act 1999 (Act No.1 of 1999)

3.9 Departmental Security Policy

## 4 SCOPE OF APPLICATION

This policy applies to the following:

4.1 All officials of the Department of Public Works, Roads and Transport.

4.2 Consultants; contractors; learners / interns or any third party authorized to use PWR&T facilities.

4.3 All IT solutions, that is, computer resources, systems and networks that are owned or leased by the Department.

## 5 POLICY STATEMENTS

### 5.1 SECURITY

### 5.1.1 Security Management

5.1.1.1 Information security shall be coordinated and supported at Senior Management level in the Department. It is the responsibility of Senior Management to support and ensure that the necessary ISS endeavours and initiatives are coordinated and enjoys the necessary privileges.

5.1.1.2 A Security and Risk Management Committee responsible for all IT security related issues shall be put in place. This shall be composed of representatives from the IT section, Risk Management Section, and Internal Audit and Security section. Representatives from other Business Units can be co-opted as and when required.

5.1.1.3 The following security management aspects shall be addressed by the Security Committee:

5.1.1.3.1 Information Security Awareness

5.1.1.3.2 Manage the Department Security Program

5.1.1.3.3 Business Continuity and Disaster Recovery
5.1.1.3.4 IS Risk Management
5.1.1.3.5 IS Audit and Review

### 5.1.2 Personnel Security

5.1.2.1 The employees of the Department accessing information systems and the data processed by the systems shall meet the necessary security requirements as determined by the sensitivity of information accessed.

5.1.2.2 Access to the systems and data shall be immediately terminated as soon as evidence of non-compliance with the security requirements is picked-up.

5.1.2.3 Information security roles and responsibilities shall be included in approved Job descriptions where required.

5.1.2.4 All employees who use IT services are required to acknowledge acceptance of and intention to comply with the Acceptable Use Policy by signing the department Information Technology User Declaration Agreement. Any employee found to have violated this policy shall be subjected to appropriate disciplinary action.

5.1.2.5 All Third Party organisations are required to sign a Non-Disclosure Agreement (NDA) before access to any IT resource/s is/are permitted.

5.1.2.6 All access to PWR&T network shall require a unique username and password.

5.1.2.7 The proper use of passwords to manage access to systems is critical.

### 5.1.3 Network Security

5.1.3.1 The SITA GCCN Security Policy shall apply for the WAN connections to PWR&T's network sites to ensure the safeguarding of information on networks and the protection of the supporting infrastructure.

5.1.3.2 Defaults accounts (guest, supervisor or administrator) shall be configured to meet the Departmental requirements.

5.1.3.3 All connections to the PWR&T's LAN shall be authorized by the HOD.

5.1.3.4 Secure remote access shall be strictly controlled. Control shall be enforced via one-time password authentication or public / private keys with strong pass-phrases.

5.1.3.5 Administrator passwords shall be kept sealed in a fireproof safe and known to at least two (2) persons.

### 5.1.4 Unlicensed Software

5.1.4.1 Under no circumstances shall illegal software be loaded on official computer equipment without prior consent from the IT Section.

5.1.4.2 The IT Section has the right to remove any such illegal software without prior notification.

### 5.1.5 Physical Security

5.1.5.1 The MISS applies. The Security policy of the Department shall be consulted for issues on physical security. All security areas / buildings where computer related equipment is used shall be classified according to its criticality in terms of risk and be protected to conform to the applicable standard of security.

5.1.5.2 Where feasible access to the Server rooms shall be strictly controlled and restricted to authorized personnel. Authentication controls like swipe cards or PIN shall be used to authenticate and validate access. An Audit trail shall be securely maintained.

5.1.5.3 Where feasible Fire prevention standards and procedures shall be established and adhered to in order to prevent fire from starting spontaneously due to negligence or as a result of arson. Fire fighting equipment, sensitive to electronic environments and thermal shock on magnetic media, shall be deployed in high-risk areas. Fire detecting sensors (heat and smoke) shall be linked to an alarm system and shall be regularly tested.

5.1.5.4 Fire fighting and evacuation procedures shall be adhered to and personnel shall be trained in the effective execution of these procedures. Regular simulations shall be conducted.

5.1.5.5 An access control system and procedures shall be implemented to control the movement of personnel and visitors on these areas.

5.1.5.6 A removal control system and procedures shall be implemented for all computer related equipment entering or leaving Departmental offices.

### 5.1.6 Server Security

5.1.6.1 All servers hosting data and applications shall be located in a physically secured environment where access is strictly controlled.

5.1.6.2 All server rooms and/or patch rooms shall be regarded as high-risk security areas and access to these areas shall be strictly controlled.

5.1.6.3 All servers shall be loaded and protected with the latest approved anti-virus software. Updates for patches and upgrades shall be implemented regularly.

5.1.6.4 Only an authorized administrator shall be granted administrative rights on the servers. Administrative password shall be kept secret and only nominated personnel at management's discretion shall have access to the password.

5.1.6.5 Servers shall be backed up in accordance with the PWR&T backup procedures.

### 5.1.7 Workstation Security

5.1.7.1 All workstations shall be located in a physically protected environment where access control measures are in place and applied consistently. It shall be ensured that unattended equipment has appropriate security protection.

5.1.7.2 Classified data shall not be stored on the local hard drive of workstations. All classified data processed using workstations shall be saved on a secure network drive on a server.

5.1.7.3 All workstations shall be loaded and protected by the latest approved Anti-Virus software.

5.1.7.4 It is the responsibility of the workstation user to ensure that appropriate security measures and practices are adhered to. Protection of the data stored on workstations is the responsibility of the workstation user.

5.1.7.5 Users shall not leave their workstations unattended while accessing or processing information without appropriate protection like password protected screen savers.

5.1.7.6 Workstations used to access classified, secret or top secret, information shall at least be protected by two-factor authentication. For example encryption, smart cards, tokens

5.1.7.7 Users shall not share workstation passwords and user accounts with anyone.

5.1.7.8 It is the responsibility of the workstation user to ensure that his/her workstation is adequately protected from logical threats as well as physical environmental threats.

5.1.7.9 Users shall ensure that all systems and data are properly backed-up and that local and network drives are synchronised.

### 5.1.8 Media Storage and Security

5.1.8 Information classified confidential, secret and top secret shall not be stored on unsecured media, like local drives of workstations, stiffy disks, mobile hard drives, CD's and email systems.

5.1.9 If needed encryption technologies shall be used to encrypt classified data stored on the network, email, and any electronic media.

5.1.10 Access to data media or facilities housing data media shall be controlled

5.1.11 Data media shall be archived / disposed of according to system design specifications and the provisions of the National Archives Act.

### 5.1.9 Password Security

#### 5.1.9.1 Strong passwords.

All user-chosen passwords for computers and networks shall be difficult to guess. Personal details such as spouse's name, car number plate, Identity number, and birthday shall not be used unless accompanied by additional unrelated characters.

### 5.1.9.2 Display and Printing of Passwords.

The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorized parties shall not be able to observe or subsequently recover them.

### 5.1.9.3 Periodic Password Changes.

All users shall be required to regularly change their passwords.

### 5.1.9.4 Changing of given Passwords.

The initial passwords issued by a security administrator shall be valid only for the involved user's first on-line session. At that time, the user shall be forced to choose another password before any other work can be done.

### 5.1.9.5 Account Lockout.

A user's account shall be locked after three unsuccessful logon attempts and only the system administrator can unlock user accounts.

### 5.1.9.6 Identification.

Users shall have a unique user name and passwords to identify them on the systems.

### 5.1.10 Acceptable Use Policy (AUP)

This AUP clause constitutes the code of conduct for all users of our IT resources.

### 5.1.10.1 Acceptable Use

5.1.10.1.1Connecting to **PWR&T IT resources is a "privilege"** and not a right.

5.1.10.1.2**"Strong passwords"** (a combination of letters, numbers, symbols and characters e.g. @-*#_$%! 1-9 Aa?{}^&) shall be used when logging in to computer resources.

5.1.10.1.3Passwords should be treated as confidential.

5.1.10.1.4Passwords should be changed regularly.

5.1.10.1.5A **"compromised password"** shall be changed immediately.

5.1.10.1.6Every computer machine should have an auto-lock login screen saver.

5.1.10.1.7Always lock your computer when you temporarily leave your desk (Press **CTL +ALT + DEL).**

5.1.10.1.8Work related documents shall be stored on the File Server.

5.1.10.1.9Every individual user **should ensure** that documents are backed-up (see Annexure. A)

5.1.10.1.10 Every official assigned with IT resources is responsible and accountable for its security.

### 5.1.10.2 Prohibited Use

5.1.10.2.1 Illegal or Unauthorized Access (hacking) to other people's computers or accounts is prohibited.

5.1.10.2.2 **Weak passwords** or easy to guess passwords.

5.1.10.2.3 The installation of **illegal or unauthorized software.**

5.1.10.2.4 The **sharing of passwords** and **user accounts.**

5.1.10.2.5 The use of PWR&T systems and networks for fraudulent activities.

5.1.10.2.6 The **tempering** with computer machines (striping and or opening)

5.1.10.2.7 Unauthorised disclosure of PWRT information.

5.1.10.2.8 The playing of multi-media applications.

5.1.10.2.9 Unauthorised viewing or browsing of files or accounts of other people.

5.1.10.2.10 **Spamming (mass e-mails)** – to be avoided or done with management permission.

5.1.10.2.11 Misuse of the E-mail system for the distribution of disruptive messages on sex, disability, religion, race etc.

5.1.10.2.12 The sending of unsolicited and or offensive e-mail messages to other people.

### 5.1.11 Encryption

5.1.11.1 All external communication over MPG WAN and / or MPG LAN to LAN communication over the WAN classified confidential, secret or top secret shall be encrypted with approved SACSA cryptographic devices before transmission.

5.1.11.2 When making use of Public Key Infrastructure (PKI), all session keys shall be transmitted in encrypted format.

5.1.11.3 Where encryption is not used for the external transmission of classified information, it shall be reported as a breach of security to the IT section.

5.1.11.4 If the Department's data classified secret or top secret is to be transported in computer-readable storage media (such as magnetic tapes, stiffy-disks, mobile hard drives, laptops or CD-ROMs), it shall be in encrypted form.

### 5.1.12 Document Security Policy

5.3.4.1 All documents, manual files, printouts shall be classified in accordance with the Minimum Information Security Standards (MISS) classification scheme. It is the responsibility of the person accessing or using the documentation to understand the sensitivity of the material contained in the documentation.

5.1.12.2 Access to highly classified documents shall be strongly controlled. Authorization from appropriate owner shall be obtained. It is the owner's responsibility to ensure that all access requirements to the documentation are satisfied as outlined by the classification requirements and security status of the recipient.

5.1.12.3 Documents and sensitive data files shall be kept in a safe environment. A backup procedure for all manuals, files and documents critical to the Department business shall be put in place to ensure the availability of information in manual file system.

5.1.12.4 Classified documents (confidential, secret or top secret) shall not be printed on network printers accessible to everyone.

5.1.12.5 Requests for access to highly classified documents shall be scrutinized and logged if granted. All sensitive documents accessed shall be accompanied by a business motivation and authorization.

5.1.12.6 Systems and Network documentation shall be classified as Secret. Access to this documentation shall be strictly controlled and only people authorized to view, change or modify the system configurations shall be allowed access to the documentation.

5.1.12.7 Systems and Network documentation shall be kept and locked away in a safe place.

5.1.12.8 Common Directories: No sensitive documents shall be stored in public directories, as these directories are made available to all users.

5.1.12.9 Common Directories: Each Common directory shall have a designated owner who is responsible for the regular cleaning out of redundant data,

### 5.1.13 Third Party Connections Security

Third Party Persons shall have access to PWRT Network approved by the HOD.

### 5.1.14 Disaster Recovery and Backups

5.1.14.1 The IT section shall work in conjunction with other network administrator bodies to ensure that preventative measures are in place. The Departmental Disaster Recovery Plan (DRP) shall incorporate IT Disaster Recovery Plans.

5.1.14.2 Data backup procedure shall be established and adhered to for all the information systems and operations.

5.1.14.3 Data backup devices shall be kept in a safe environment offsite the building where they can be accessible with ease when needed.

### 5.1.15 IT Change Management

5.1.15.1 A formal change management process shall be established including approval of change requests.

5.1.15.2 All changes shall be done in accordance with an approved change management process of the Department

### 5.1.16 Implementation and Testing

5.1.16.1 All approved changes shall be monitored to ensure that they are implemented according to specification.

5.1.16.2 The effects of changes shall be analysed before changes are approved and implemented.

5.1.16.3 It is the responsibility of management to ensure that all approved changes to critical IT resources are at a minimal level of risk to the IT infrastructure.

### 5.1.17 Firewall (ITB's responsibility)

5.1.17.1 Information Technology Management shall tightly control the physical access to the firewalls, allowing only the firewall administrators and network services manager physical access to the servers.

5.1.17.2 The Firewall Administrator is responsible for Firewall configuration tables to determine what is permitted in or denied.

5.1.17.3 Rules shall be established as to which incoming and outgoing services shall be denied or allowed for various client/servers (e-mail, ftp, telnet, www, etc).

5.1.17.4 Standards shall be established to stipulate which service utilizes specific port numbers. All services and connections through the firewall shall be denied unless specifically permitted by the Network Administrator.

5.1.17.5 The firewall shall log all reports on daily, weekly, and monthly bases to allow the analysis of the network activity through the firewall.

5.1.17.6 Firewall administrators shall audit the firewall logs in a timely manner (daily, if possible) to detect possible attacks from the Internet.

5.1.17.7 Threat and vulnerability analysis shall be performed continuously (3 months).

## 5.2 INFORMATION TECHNOLOGY

### 5.2.1 Procurement of IT Solutions

5.2.1.1 All applications to acquire IT solutions shall be submitted to the Departmental Information Technology Committee (DITC) (See Annexure C)

5.2.1.2 SITA contracts shall be used for all procurement unless otherwise permitted by the HOD as recommended by the DITC.

5.2.1.3 All services rendered shall be governed by SLA's that conform to Departmental Security Standards

### 5.2.2 Management and Usage of IT Solutions

5.2.2.1 It is the sole responsibility of IT officials to configure, install and repair IT solutions. No any other official is allowed to temper with IT solutions.

5.2.2.1 The IT section's responsibility is to ensure that all IT solutions are functional and used properly by the Department.

### 5.2.3 The user's responsibilities include:

5.2.3.1 To ensure that IT solutions allocated to individuals are secured against loss by theft, fraud, malicious or accidental damage and any other illegal activity.

5.2.3.2 To report to IT section any faults or malfunctioning or any suspicious activity occurring on the IT solution.

### 5.2.4 Management of IT incidents

5.2.4.1 An Incident Management team shall be formed to execute the following tasks:

5.2.4.1.1 Receive notification of incidents.

5.2.4.1.2 Investigate incidents.

5.2.4.1.3 Draft a report providing detail of the incident and accompanying evidence.

5.2.4.1.4 Report the findings to the HOD immediately.

5.2.4.1.5 Escalate all incidents affecting information systems to IT

5.2.4.1.6 Escalate all incidents affecting physical security to the Security Manager.

5.4.4.1.7 Incidents include the following:

5.4.4.1.7.1 Network attacks
5.4.4.1.7.2 Denial of services
5.4.4.1.7.3 Theft
5.4.4.1.7.4 Infrastructure compromise
5.4.4.1.7.5 Virus infections
5.4.4.1.7.6 Availability and integrity compromise

5.4.4.1.7.7 Fraud
5.4.4.1.7.8 Illegal activity
5.4.4.1.7.9 Incident that requires investigation of electronic documents

### 5.2.5 Private Equipment

Private equipment shall only be allowed for PWR&T's legitimate business needs (see annexure B)

### 5.2.6 Electronic Mail (ITB Policy applies)

5.2.6.1 As a productivity enhancement tool, the department encourages the business use of electronic communications. Electronic communications systems, and all messages that are generated on or handled by electronic communications systems, including backup copies, are considered to be the property of MPG.

5.2.6.2 MPG electronic communications systems generally shall be used only for business purpose. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

5.2.6.3 Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation and related information that are included with electronic messages or postings shall reflect the actual originator of the messages or postings.

5.2.6.4 The department management shall regularly monitor the content of electronic communications. Content and usage of electronic communications shall be monitored to support operational, maintenance, auditing, security and investigative activities.

5.2.6.5 Recognizing that some information is intended for specific individuals and shall not be appropriate for general distribution, electronic communications users shall exercise caution when forwarding messages. The Department sensitive information shall not be forwarded to any party outside PWR&T without the prior approval of IT & RM Manager.

5.2.6.6 Users shall be aware of the classification of any information contained in data files or correspondence which they are transporting using email communication and do not exchange information in un-encrypted form which is confidential.

### 5.2.7 Internet Policy (ITB Policy applies)

5.2.7.1 Access to the Internet shall be granted to employees that have a legitimate need for such access, the user needs to apply for access formally through the respective line manager and the Chief Director Corporate Services shall approve the request.

5.2.7.2 All Internet connections shall be via the approved Internet service provider of the department. Any other connections are prohibited.

5.2.7.3 Use of Internet is a privilege, which constitutes the acceptance of responsibilities, and obligations that are subject to government policies and laws. Acceptable use shall be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanism and individual rights to privacy from intimidation, harassment and annoyance.

5.2.7.4 All users shall authenticate themselves at MPG internal Web proxy server before gaining access to the Internet. This authentication process shall be achieved by logging on to the Internet via user name and password system.

5.2.7.5 To protect MPG from profane material and to minimize the use of bandwidth, all Internet usage shall be monitored by Web content filtering software.

5.2.7.6 Misrepresenting, obscuring, suppressing or replacing the identity of a user on the Internet or any MPG communication systems is forbidden.

5.2.7.7 Users shall not publicly disclose internal PWR&T information via the Internet, which could adversely affect PWR&T, customer relations or public image.

5.2.7.8 Users shall be subject to limitations on their use of the Internet as determined by the appropriate supervising authority.

5.2.7.9 MPG content filtering software shall prevent users from connecting to certain non-business web sites. All web sites that contain sexually explicit, profane and other potentially offensive material shall be blocked out via the proxy server.

5.2.7.10 At any time and without prior notice, the Department management reserves the right to examine Web browser cache files, Web browser bookmarks and other information that is stored on or passing through the computers of the Department. Such management access assures compliance with internal policies, assists with internal investigations and assists with the management of the Department.

## 6. ROLES AND RESPONSIBILITIES

6.1 The HOD for PWR&T is accountable for this policy and shall ensure adherence thereto.

6.2 The GM: Integrated Planning is accountable for the implementation and enforcement of this policy.

6.3 The Senior Manager: Knowledge Management is responsible for the implementation and enforcement of this policy.

6.4 System Owners are responsible for ensuring that appropriate security controls are implemented.

6.5 The IT section shall ensure compliance of the IT policy.

## 7. MONITORING AND EVALUATION

The IT section shall monitor the implementation of the policy and shall report any deviations to the Head of the Department.

## 8. POLICY REVIEW

The policy shall be reviewed to factor in changes in legal frameworks, organizational development, political and economic trends, and envisaged outputs by the Medium Term Expenditure Framework as well as outcomes of monitoring and evaluation.

## 9. APPROVAL

Approved

**KM MOHLASEDI**
**HEAD OF DEPARTMENT**

**DATE** : 26/06/2012

## Annexure A

## PROCEDURE: BACKUP

### INTRODUCTION

This document explains how to make a pc backup on the local drive. Information or data gets backed up once a week or daily. When the pc fails, this data can be used to restore the pc back to its original state.

### 1. General Backup Guidelines

1.1 Ensure that your backup device is ready to record the data
1.2 Select the location where files are stored and copy
1.3 Choose a location to save the backup and paste
1.4 When the backup is finished keep the storage devices off-site

### 2. Daily Personal Computer Backup Procedure

It is the responsibility of every official to ensure that all the information / data in their computers is backed up

2.1 Users shall save all their official files on "My documents folder"
2.2 The IT section shall be consulted for assistance on all backup technicalities

Note that preferred media for this backup shall be data / writable disk or memory sticks.

**Annexure B**

## PROCEDURE: ACCESS CONTROL

**NB:** All Access Control Forms (e.g. E-mail, Internet, Network access etc) are obtainable from the IT section.

### 1. Network Access

1.1 Complete Network Application Form
1.2 Submit the completed form
1.3 An Account with a unique Username shall be issued
1.4 The HOD's approval is required only for private users

### 2. E-mail and Internet Access

The E-mail and Internet facilities are being offered and managed by the Provincial ITB. The following procedure shall be adhered to:

2.1 Complete the E-mail (or internet form for internet) application form(s).
2.2 Submit the completed application form(s).
2.3 An E-mail (or Internet) account shall then be issued.

**NB:** In case of the Internet the application form shall be sent for approval before submission.

Accessing the forms

1 The "e-mail application form" comes with the e-mail policy. It can be downloaded from Part's Website pwrt.mpu.gov.za/roads/systems.htm

2 The "internet application form" comes with the internet policy. It can be downloaded from pwrt's website pwrt.mpu.gov.za/roads/systems.htm

**Annexure C**

## PROCEDURE: ACQUISITION OF IT SOLUTIONS

Departments shall manage information technology effectively and efficiently. The Batho Pele principle of offering equal access to services, increase in productivity and lowering of cost, shall inform the acquisition, management and use of information technology. Information technology shall be used as a tool to leverage service delivery by the public service and shall therefore not be acquired for its own sake.

All applications to acquire/purchase IT solutions shall be submitted to Departmental Information Technology Committee for approval.

1. The following process shall be followed acquiring of IT solutions:

1.1 Request for Quotation
1.2 Complete an application form
1.3 Submit Completed Form

2. Note in case of replacements, the following process applies

2.1 Request IT assessment report
2.2 Repeat step 1, 2 and 3

3. Note that all documents for the above processes are obtainable from IT section

**Desktops**

1. The provision of desktop computers to officials shall depend on the need for such equipment.
2. The following PC types will be considered for applications by the DITC

3.1 Entry level range (small size files).
3.2 Middle range (office applications & transversal systems).
3.3 Specialist range (graphics and sophisticated workloads).

3. If an official is currently in possession of a desktop computer, he/she has to provide an IT Report with the DITC form to explain what is wrong with the current computer.

**Laptops**

4. The provision of laptop to officials shall depend on the need for such equipment.
5. The following laptop types shall be considered for applications by the DITC

5.1 Entry level range (small size files).
5.2 Middle range (office applications & transversal systems).
5.3 Specialist range (graphics and sophisticated workloads).

6. If an official is currently in possession of a laptop computer, he/she has to provide an IT Report with the DITC form to explain what is wrong with the current laptop.

**Printers**

1. The provision of printer to officials shall depend on the need for such equipment.

2. The provision of a new printer has to be first checked, as to whether the possibility of shared printer exists in case of open space offices.

3. The following laptop types shall be considered for applications by the DITC

3.1 Entry level range (small size files).
3.2 Middle range (office applications & transversal systems).
3.3 Specialist range (graphics and sophisticated workloads).

4. If an official is currently in possession of a printer, he/she has to provide an IT Report with the DITC form to explain what is wrong with the current printer.

**Systems OR Servers**

1. The provision of servers to officials shall depend on the need for such equipment.
2. The provision of systems or servers shall depend on the system or server needs.
3. The IT section shall be involved in the following procurement processes

3.1 Request for Proposals
3.2 Technical Evaluation
3.3 Drawing and Signing of SLA
3.4 Steering Committee

**Shared or Pool devices**

1. The provisioning of the following devices shall require a motivation indicating why sharing will not work.
2. The following are some of the devices that shall be shared:

2.1 Projectors
2.2 Digital cameras
2.3 Flatbed scanners
2.4 Dictaphone
2.5 Laptops
2.6 Desktops
2.7 Printers, etc

Annexure D

## PROCEDURE: DISPOSAL OF IT SOLUTIONS

1. The purpose of this procedure is to provide guidelines for the proper disposal of all the retired or obsolete IT solutions in the Department of Public Works Roads and Transport.

2. This procedure applies to all the IT solutions in the Department (e.g. Hardware and software). All leased IT solutions shall be erased of all departmental information before returning to the lessor.

3. A notification for disposal shall be made to the IT section; the notification can either be verbal or written. The notification shall have at least the following information:

   3.1 Details of the owner (e.g. name and telephone number)
   3.2 Location of the equipment
   3.3 Serial number
   3.4 Warranty / guarantee status
   3.5 Valid reason for disposal

4. An IT technician shall conduct an assessment and recommend with reasons an action to be taken with regards to the IT solution. If equipment is recommended for disposal the following process shall apply:

   4.1 Ensure valuable data is removed and stored in a network storage
   4.2 Clean all the data in memory (Disk Sanitizer )
   4.3 Complete a data cleansing audit form
   4.4 Information be stored for a maximum period of 12 months

**Annexure E**

## DEPARTMENTAL SYSTEMS

1. The following two categories classify all systems as used by PWR&T users:

   1.1 Transversal Systems
   1.2 Non-Transversal Systems

2. The following is a list of systems and functions used by the Department.

| | |
|---|---|
| **BAS** | Creditors and Bookkeeping |
| **DRONE** | Project Management |
| **e-NATIS** | Registration of Vehicle Licences |
| **GIS** | Management and display of spatial data (projects / assets) |
| **IEWORKS** | Management of Immovable Asset (Property) |
| **LOGIS** | Procurement |
| **LPRO** | Computerized Learners Testing System |
| **LTPS** | Implementation of National Land Transport Act |
| **NLTIS** | Implementation of National Land Transport Act |
| **PERSAL** | Personnel and Salary Administration |
| **PMIS** | Project Management |
| **RAMS** | Road Asset Management System |